Risk Management: Law and Practice

風險管理：法律與常規

A Google search on the term 'risk management' returns 4,260 million results in 0.38 seconds as compared with 'Xi Jingping' with 63.4 million results in 0.35 seconds. Risk management is important from nations to companies to professional bodies. On the national front, President Xi has already warned back in 2019 to 'alert to Black Swan and prevent Gray Rhino' in managing risks and events confronting China. This FRA column will focus on the law and practice (including procedures) relating to risk management that are relevant to (a) companies (particularly companies listed on Hong Kong Stock Exchange (HKEX)) and (b) professionals (with reference to law firms and solicitors).

Risk Management for Companies under Companies Ordinance

Under section 388 of the Companies Ordinance (Cap. 622), directors of a Hong Kong company are required to prepare for each year a report that complies with (amongst other things) Schedule 5 to the Companies Ordinance. Schedule 5 prescribes the contents of the directors' report as regards business review. Under paragraph 1(b) of Schedule 5, a directors' report for a financial year must contain a business review that consists of 'a description of the principal risks and uncertainties facing the company'. In short, a company is required to address risk management in its business review under the Companies Ordinance.

Under paragraph 28(2)(d) of Appendix 16 of the Main Board Listing Rules (relating to the disclosure of financial information), a listed company (whether or not it is incorporated in Hong Kong) shall include disclosures required under Schedule 5 to the Companies Ordinance, including, the description of the principal risks and uncertainties facing a listed company.

Under the law and/or the Listing Rules, a Hong Kong company or a non-Hong Kong company listed on HKEX is required to disclose the principal risks and uncertainties facing that company under paragraph 1(b) of Schedule 5 to the Companies Ordinance.

Risk Management for Listed Companies under Main Board Listing Rules

For all companies listed on HKEX, they are subject and are required to comply with the Listing Rules including the Corporate Governance Code (CG Code) under Appendix 14 of the Listing Rules. Under the CG Code, the requirements are set out as (a) principles of good corporate governance (Principle), (b) code provisions (CPs) and (c) recommended best practices (RBPs). Under the comply or explain regime, CPs are required to be complied or explained with their non-compliance by listed companies. RBPs are not required to be complied nor explained but are encouraged to do so. Risk management and internal control are prescribed and regulated under D2 of the CG Code with one (1) Principle, seven (7) CPs (CP D.2.1 – D.2.7) and two (2) RBPs (RBP D.2.8 and D.2.9).

Under the Principle, it provides that 'the board is responsible for evaluating and determining the nature and extent of the risks it is willing to take in achieving the [listed company's] strategic objectives, and ensuring that the [listed company] establishes and maintains appropriate and effective risk management and internal control

在谷歌上搜尋「風險管理」一詞，系統會在0.38秒內顯示出42.6億條結果，而搜尋「習近平」可在0.35秒內得到6,340萬條結果。不論對國家、公司，乃至專業機構而言，風險管理均至關重要。在國家層面，習主席早於2019年已警告中國在管理風險事件時，須「警惕黑天鵝，防範灰犀牛」。本期《財經事務及監管政策委員會》專欄將聚焦於與（a）公司（尤其於香港交易所（港交所）上市的公司）及（b）專業人士（以律師行及律師為例）業務相關的風險管理相關法例及常規。

《公司條例》下的企業風險管理

根據《公司條例》（第622章）第388條，香港公司董事須就每個年度擬備符合（其中包括）《公司條例》附表5規定的報告。附表5訂明董事報告中有關業務審視的內容。根據附表5第1(b)段，財政年度的董事報告須載有包含「對公司面對的主要風險及不明朗因素的描述」的業務審視章節。簡而言之，根據《公司條例》，公司必須於其業務審視章節中闡述風險管理事宜。

根據《主板上市規則》附錄16第28(2)(d)段（關於財務資料的披露），上市公司（不論是否在香港註冊成立）須披露《公司條例》附表5規定的資料，包括上市公司面對的主要風險及不明朗因素的描述。

根據法律及/或《上市規則》，香港公司或於港交所上市的非香港公司，須根據《公司條例》附表5第1(b)段披露公司面對的主要風險及不明朗因素。

上市公司於《主板上市規則》下的風險管理規定

所有於港交所上市之公司，須遵守《上市規則》並受其規管，包括《上市規則》附錄14《企業管治守則》。根據《企業管治守則》，所載之規定分為(a)良好企業管治的原則（「原則」）、(b)守則條文及(c)建議最佳常規。在「不遵守就解釋」機制下，上市公司必須遵守守則條文或對其偏離守則規定之情況作出解釋。概無規定要求上市公司遵守建議最佳常規或就有關偏離作出解釋，但建議上市公司加以遵守。《企業管治守則》D2條對風險管理及內部監控作出了規定及規範，包括一(1)項原則、七(7)條守則條文（守則條文D.2.1條至D.2.7條）及兩(2)項建議最佳常規（建議最佳常規D.2.8條及D.2.9條）。

原則中列明，「董事會負責評估及釐定[上市公司]達成策略目標時所願意接納的風險性質及程度，並確保[上市公司]設立及維持合適及有效的風險管理及內部監控系統。上述風險包括但不限於與環境、社會及管治有關的重大風險。董事會應監督管理層對風險管理及內部監控系統的設計、實施及監察，而管理層應向董事會提供有關系統是否有效的確認」。

守則條文中列明以下規定：根據D.2.1條，「董事會應持續監督[上市公司]的風險管理及內部監控系統，並確保最少每年檢討一次[上市公司]及其附屬公司的風險管理及內部監控系統是否有效，並在《企業管治報告》中向股東匯報已經完成有關檢討。有關檢討應涵蓋所有重要的監控方面，包括財務監控、運作監控及合規監控」。

systems. Such risks would include, amongst others, material risks relating to ESG [Environmental, Social and Governance]. The board should oversee management in the design, implementation and monitoring of the risk management and internal control systems, and management should provide a confirmation to the board on the effectiveness of these systems'.

Under CPs, the following are provided. Under D.2.1, 'the board should oversee the [listed company's] risk management and internal control systems on an ongoing basis, ensure that a review of the effectiveness of the [listed company's] and its subsidiaries' risk management and internal control systems has been conducted at least annually and report to shareholders that it has done so in its Corporate Governance Report. The review should cover all material controls, including financial, operational and compliance controls'.

Under D.2.2, 'the board's annual review should, in particular, ensure the adequacy of resources, staff qualifications and experience, training programmes and budget of the [listed company's] accounting, internal audit, financial reporting functions, as well as those relating to the [listed company's] ESG performance and reporting'.

Under D.2.3, 'the board's annual review should, in particular, consider: (a) the changes, since the last annual review, in the nature and extent of significant risks (including ESG risks), and the [listed company's] ability to respond to changes in its business and the external environment; (b) the scope and quality of management's ongoing monitoring of risks (including ESG risks) and of the internal control systems, and where applicable, the work of its internal audit function and other assurance providers; (c) the extent and frequency of communication of monitoring results to the board (or board committee) which enables it to assess control of the [listed company] and the effectiveness of risk management; (d) significant control failings or weaknesses that have been identified during the period. Also, the extent to which they have resulted in unforeseen outcomes or contingencies that have had, could have had, or may in the future have, a material impact on the [listed company's] financial performance or condition; and (e) the effectiveness of the [listed company's] processes for financial reporting and [Listing Rules] compliance'.

Under D.2.4, '[listed companies] should disclose, in the Corporate Governance Report, a narrative statement on how they have complied with the risk management and internal control code provisions during the reporting period'.

Under D.2.5, 'the [listed company] should have an internal audit function'.

Under D.2.6, 'the [listed company] should establish a whistleblowing policy and system for employees and those who deal with the [listed company]…to raise concerns, in confidence and anonymity, with the audit committee… about possible improprieties in any matter related to the [listed company]'.

Under D.2.7, 'the [listed company] should establish policy and system that promote and support anti-corruption laws and regulations'.

根據D.2.2條，「董事會每年進行檢討時，應確保［上市公司］在會計、內部審核、財務匯報職能方面以及與［上市公司］環境、社會及管治表現和匯報相關的資源、員工資歷及經驗，以及員工所接受的培訓課程及有關預算是足夠的」。

根據D.2.3條，「董事會每年檢討的事項應特別包括下列各項：(a) 自上年檢討後，重大風險（包括環境、社會及管治風險）的性質及嚴重程度的轉變、以及［上市公司］應付其業務轉變及外在環境轉變的能力；(b) 管理層持續監察風險（包括環境、社會及管治風險）及內部監控系統的工作範疇及素質，及（如適用）內部審核功能及其他保證提供者的工作；(c) 向董事會（或其轄下委員會）傳達監控結果的詳盡程度及次數，此有助董事會評核［上市公司］的監控情況及風險管理的有效程度；(d) 期內發生的重大監控失誤或發現的重大監控弱項，以及因此導致未能預見的後果或緊急情況的嚴重程度，而該等後果或情況對［上市公司］的財務表現或情況已產生、可能已產生或將來可能會產生的重大影響；及(e)［上市公司］有關財務報告及遵守［《上市規則》］規定的程序是否有效」。

根據D.2.4條，「［上市公司］應在《企業管治報告》內以述形式披露其如何在報告期內遵守風險管理及內部監控的守則條文」。

根據D.2.5條，「［上市公司］應設立內部審核功能。」

根據D.2.6條，「［上市公司］應制定舉報政策及系統，讓僱員及其他與［上市公司］有往來者…可暗中及以不具名方式向審核委員會…提出其對任何可能關於［上市公司］的不當事宜的關注。」

根據D.2.7條，「［上市公司］應制定促進和支持反貪污法律及規例的政策和系統」。

建議最佳常規方面，D.2.8條規定，「董事會可於《企業管治報告》中披露已取得管理層對［上市公司］風險管理及內部監控系統有效性的確認」。

D.2.9條規定，「董事會可於《企業管治報告》中披露任何重要關注事項的詳情。」

上述涉及根據《主板上市規則》於主板上市的公司，適用於GEM上市公司的《GEM上市規則》亦載有類似條文。

適用於律師的風險管理規定

香港律師的學歷、資格、培訓及執業均受《法律執業者條例》（第159章）規管。在風險管理教育方面，律師會理事會已根據《法律執業者條例》第73條採納《法律執業者（風險管理教育）規則》（第159Z章）（《風險管理教育規則》），實施一項關於風險管理的訓練計劃，名為「風險管理教育計劃」，適用於所有律師、實習律師及外地律師。

根據《風險管理教育規則》第5條，任何人若成為律

For RBPs, under D.2.8, 'the board may disclose in the Corporate Governance Report that it has received a confirmation from management on the effectiveness of the [listed company's] risk management and internal control systems'.

Under D.2.9, 'the board may disclose in the Corporate Governance Report details of any significant areas of concern'.

The above relate to companies listed on the Main Board under the Main Board Listing Rules and similar provisions are contained in the GEM Listing Rules for companies listed on GEM.

Risk Management for Solicitors

The qualification, admission, training and practice of Hong Kong solicitors are subject to and regulated by the Legal Practitioners Ordinance (Cap. 159). In relation to risk management education, the Council of the Law Society has pursuant to section 73 of the Legal Practitioners Ordinance adopted the Legal Practitioners (Risk Management Education) Rules (Cap. 159Z) (RME Rules) to implement a programme of training on risk management known as the 'Risk Management Education (RME) Programme' applicable to all solicitors, trainee solicitors and foreign lawyers.

Under section 5 of the RME Rules, a person who becomes a solicitor, a trainee solicitor or a foreign lawyer is required to complete all general RME core courses within the practice year. Under section 6, a solicitor who becomes a principal is required to complete all general RME core courses within the practice year. For the purpose of the RME Rules, risk management is defined as 'any action or plan of action the objective of which is to minimize the risk of a person's exposure to claims against him in the course of his professional practice and to reduce the extent of loss which may arise from such claims'. RME course means any workshop, lecture, seminar, course, programme of instruction or any other activity conducted by the Law Society or by any entity authorised by the Law Society.

Under section 7, a solicitor or a foreign lawyer is required to complete at least 3 hours of elective RME courses within the practice year failing which he is required to complete at least 6 hours of elective RME courses within that practice year and the first succeeding year. Under section 8A, the Law Society may grant exemption. Under section 9, solicitors are required to keep record of completion of RME courses and to make the records available to the Law Society for inspection.

Under the RME Rules, RME courses are not defined and specified and will deem to be RME courses if conducted by the Law Society or authorised by the Law Society. Accordingly, the RME courses that are currently offered are quite diversified that some RME courses are not technically related to risk management. In addition, the RME Rules are only applicable to solicitors and foreign lawyers individually and not applicable to law firms. Law firms are not required to prepare and submit any risk management reports to the Law Society.

師、實習律師或外地律師，須在執業年度內完成所有風險管理教育一般必修課程。根據第6條，任何律師若成為主管，須在執業年度內完成所有風險管理教育一般必修課程。就《風險管理教育規則》而言，風險管理指「任何行動或行動方案，其目標是把某人在其專業執業過程中遭申索的風險減至最低，以及減少因該等申索而可能引致的損失的程度」。風險管理教育課程指由律師會或其授權的任何實體舉辦之任何研習班、講座、研討會、課程、指導計劃或任何其他活動。

根據第7條，律師或外地律師須於執業年度內完成至少共3小時的選修風險管理教育課程，否則須在執業年度及隨後首個年度內完成至少共6小時的選修風險管理教育課程。根據第8A條，律師會可批予豁免。根據第9條，律師須保留其完成風險管理教育課程的紀錄，並可供律師會審查。

《風險管理教育規則》並未對風險管理教育課程進行界定或指定，只要課程由律師會或其授權之實體舉辦，均會被視為風險管理教育課程。因此，目前開設的風險管理教育課程頗為多樣化，有些課程在技術上與風險管理無關。此外，《風險管理教育規則》僅適用於個人律師或外地律師，並不適用於律師事務所。律師事務所無須編製並向律師會提交任何風險管理報告。

Risk Management Practice

Currently, there are two risk management frameworks that are commonly adopted for risk management, namely,

(a) Enterprise Risk Management – Integrated Framework developed by COSO (COSO Framework); and

(b) ISO 31000 Risk Management – Principles and Guidelines developed by ISO.

In Hong Kong, the COSO Framework is more popular and is adopted and used by many listed companies in preparing their risk management and internal control reports under and for the purpose of Listing Rules.

As regards risk management practice, the following are standard procedures, namely,

(a) identification of risks and risk factors;
(b) assessment of risks; and
(c) control and management of risks.

Identification of Risks and Risk Factors

Contrary to the popular understanding, risk factors were not first used in management context but were first appeared in medical context in assessing risks in heart attack based on risk factors that were identified under the Framingham Heart Study in 1948. Today, Framingham Risk Score is still used to assess 10-year risk of heart attack or death based on your age, sex, smoking habit, cholesterol and blood pressure. In company perspective, different industries and different companies will have different risks and risk factors that are required to be identified. Common risks faced by companies are strategic risk, compliance risk, financial risk, operational risk, domestic and international market risk and competitive risk. In addition, a company must bear in mind Black Swan risks and Gray Rhino risks. A Black Swan is a highly improbably major risk event that diverges beyond what is normally expected and is extremely difficult to predict with a massive impact. The Gray Rhino concept refers to risks with a high chance of occurring and a massive impact if they happen, but companies fail to recognize them as threats and overlook their obviousness.

Assessment of Risks

Once the risks are identified, they will be measured and assessed. Risks may be assessed qualitatively by professional judgement or quantitatively by risk assessment models, the most common of which is the Monte Carlo simulation and risk analysis model. In Hong Kong, most risks are assessed by the directors based on their professional judgement and business acumen. After assessment, the risks are classified into low, medium and high risks with low, medium and high financial and operational impacts. This likelihood (of risk occurrence) and impact (financial or operational) is then contained in the likelihood and impact grid. A company will focus its attention on the risks with high occurrences and high financial impacts. Whether and to what extent a company will undertake a risky event will depend on its risk philosophy and its risk tolerance and appetite.

風險管理常規

目前，風險管理普遍採用兩種風險管理框架，分別為：

(a) 全美反舞弊性財務報告委員會發起組織委員會（COSO）公佈的《企業風險管理 — 整合框架》（COSO框架）；及

(b) 國際標準組織制定的 ISO 31000 風險管理 — 原則和指導方針。

COSO 框架在香港較為普遍，眾多上市公司根據《上市規則》編製風險管理及內部監控報告時，均會採用該框架。

在風險管理常規方面，以下為標準程序，即：

(a) 識別風險及風險因素；
(b) 進行風險評估；及
(c) 監控及管理風險。

識別風險及風險因素

有別於大眾的理解，風險因素最初並未應用於管理領域，而是最初出現於醫學領域，其於1948年的「Framingham心臟研究」(Framingham Heart Study) 中首次出現，當時研究中識別出的風險因素，用於評估心臟病發作的風險。如今，醫療領域中仍會根據患者的年齡、性別、吸煙習慣、膽固醇及血壓，並運用Framingham風險評分，為患者進行十年心臟病發作或死亡評估。於企業層面而言，各行業及企業需要識別的風險和風險因素各不相同。企業面對的常見風險包括策略風險、合規風險、財務風險、營運風險、國內外市場風險及競爭風險。此外，企業須警惕黑天鵝及灰犀牛風險。黑天鵝指發生機會率極低且超出預期的重大風險事件，一般難以預料，並會造成巨大影響。灰犀牛的概念指發生機會率高、且一旦發生將造成巨大影響的風險事件，但企業往往未能認識到其威脅，並忽略這類顯而易見的危機。

進行風險評估

識別風險後，需要對其進行衡量及評估。企業可透過專業判斷對風險進行定性評估，亦可透過風險評估模型進行定量評估，其中最廣為人知的是蒙地卡羅模擬法及風險分析模型。在香港，企業主要由董事以其專業判斷及商業頭腦，對風險進行評估。風險評估分類為低、中、高風險，其分別對財務及運營狀況造成低、中、高程度的影響。（風險發生的）概率及（對財務或業務狀況的）影響，將列於概率及影響表格中。企業將聚焦於發生概率高、對財務影響較大的風險。一家企業是否進行風險活動以及其進行的程度，將取決於其風險管理理念及其風險承受能力和偏好。

監控及管理風險

識別及評估風險後，企業需就該等風險採取應對措施，包括迴避風險（或若可行的話，消除風險）、降低風險（或緩減風險）、分擔風險（或若可行的話，轉移風險）或承受風險。一般情況下，企業會承受低風險或對

Control and Management of Risks

Once the risks are identified and assessed, a company will respond to those risks, including, risk avoidance (or risk elimination, if possible), risk reduction (or risk mitigation), risk sharing (or risk transfer, if possible) or risk acceptance. Normally, a company will accept an event with a low risk or low financial impact and will avoid an event with a high risk or high financial impact. In between, directors will consider ways and means to control and manage those risks. Control activities are activities undertaken by a company to reduce or mitigate the inherent risks so that after taking such measures, the residual risks are reduced or mitigated to a level that is acceptable to such company. The control activities taken will depend on the nature of the event, the risks associated with such event, and the risk profile and philosophy of such company.

After the risks of the company are identified and assessed with control activities taken, a risk management report will be prepared and approved by the board of the company. The risk management report will be reviewed and updated on a regular basis to see if there is any change as regards the company's risk profile and risk management.

For solicitors and others who are subject to the RME Rules, they are only required to attend RME courses as required of them or perform other RME activities that are approved by the Law Society. They are not required to submit any report of their RME activities to the Law Society but are required to declare their compliance with the RME Rules when applying for their practising certificates (to enable them to practise law in Hong Kong under the Legal Practitioners Ordinance). M

Vincent P C Kwan
Solicitor/Certified Public Accountant (Fellow) (Non-Practising)
Master of Medical Sciences (Distinction) (HKU MED)
Member (Formerly Chairman), FRA Committee
The Chamber of Hong Kong Listed Companies

財務影響較低的事件，並迴避高風險或對財務影響較大的事件。若程度於兩者之間，則董事將考慮如何監控及管理該等風險。監控活動指企業為降低或緩減固有風險而採取的措施，其目的是在實行措施後，將剩餘風險降低或緩減至企業可接受的水平。企業所採用的管控措施將取決於事件的性質及風險，以及該企業的風險狀況及理念。

在識別及評估企業的風險，並採取管控措施後，企業須編製風險管理報告，以及將其提交予董事會批核。企業將定期審核及更新風險管理報告，以了解其風險狀況及風險管理是否有任何變動。

須遵守《風險管理教育規則》的律師及其他人士，僅須按規定參加風險管理教育課程，或參與律師會批准之其他風險管理教育活動。他們毋須就其參與的風險管理教育活動，向律師會提交任何報告，但須在申請執業證書時（使其可根據《法律執業者條例》於香港執業），聲明已遵守《風險管理教育規則》。M

關保銓
律師 / 資深會計師（非執業）
醫療科學碩士（優等）（香港大學醫學院）
香港上市公司商會
財經事務及監管政策委員會委員（及前任主席）